WHAT IS CLAIMED IS:

1. An information recording medium comprising:

validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information; and

information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data.

2. An information recording medium according to claim 1, wherein said validity data and said information to be validated form an electronic ticket.

3. An information recording medium according to claim 2, wherein said information to be validated further comprises content of rights associated with the electronic ticket.

4. An information recording medium according to claim 3, wherein said information to be validated is processed so as to be prevented from being tampered with.

5. An information recording medium according to claim 4, wherein said information to be validated includes a digital signature so as to be prevented from being tampered with.

6. An information recording medium according to claim 3, wherein said validity data further comprises the number of uses of the electronic ticket.

7. An information recording medium according to claim 1, wherein said validity data is encrypted.

8. An information recording medium according to claim 7, wherein said validity data is encrypted with a predetermined key, and said predetermined key is encrypted with another key.

9. An information recording medium according to claim 2, wherein the secret information is a secret key used in a public key cryptosystem, and the verifying parameter is a public key corresponding to the secret key.

10. An information recording medium according to claim 2, wherein said information to be validated further comprises an issuer certificate including issuer identifying

information for identifying an issuer of the electronic ticket, a public key for verifying the issuer, and a digital signature generated by a predetermined certifying center for the issuer identifying information and the public key, thereby certifying the issuer of the electronic ticket.

11. An information processing apparatus comprising:

validity-data generating means for generating validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information;

verifying-parameter generating means for generating a verifying parameter for verifying the presence of the secret information;

information-to-be-validated generating means for generating information to be validated which includes the verifying parameter and which is validated by the validity data; and

output means for outputting a set of information consisting of the validity data and the information to be validated.

12. An information processing apparatus according to claim 11, wherein said set of information forms an

electronic ticket.

13. An information processing apparatus according to claim 12, wherein said information-to-be-validated generating means generates the information to be validated which further includes content of rights associated with the electronic ticket.

14. An information processing apparatus according to claim 13, wherein said information-to-be-validated generating means processes the information to be validated so as to prevent the information to be validated from being tampered with.

15. An information processing apparatus according to claim 14, wherein said information-to-be-validated generating means processes the information to be validated by adding a digital signature to the information to be validated, thereby preventing the information to be validated from being tampered with.

16. An information processing apparatus according to claim 12, wherein said output means performs authentication processing with an external device when outputting the validity data and the information to be validated to said

external device.

17. An information processing apparatus according to claim 12, wherein said output means encrypts the validity data and then outputs the encrypted validity data.

18. An information processing apparatus according to claim 17, wherein said output means sends a device certificate to an external device, said device certificate including a public key used in a public key cryptosystem, and a digital signature generated by a predetermined certifying center for the public key so as to certify that said information processing apparatus is a legal device, and said output means decrypts, by using a secret key corresponding to the public key, an encryption key which is encrypted with the public key contained in the device certificate and which is sent from said external device, and encrypts the validity data with the decrypted encryption key.

19. An information processing apparatus according to claim 12, wherein said validity-data generating means generates the validity data which includes a secret key in a public key cryptosystem as the secret information, and said verifying-parameter generating means generates a public key corresponding to the secret key as the verifying parameter.

20. An information processing apparatus according to claim 12, wherein said information-to-be-validated generating means generates the information to be validated which further comprises an issuer certificate including issuer identifying information for identifying an issuer of the electronic ticket, a public key for verifying the issuer, and a digital signature generated by a predetermined certifying center for the issuer identifying information and the public key, thereby certifying the issuer of the electronic ticket.

21. An information processing method comprising:

a validity-data generating step of generating validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information;

a verifying-parameter generating step of generating a verifying parameter for verifying the presence of the secret information;

an information-to-be-validated generating step of generating information to be validated which includes the verifying parameter and which is validated by the validity data; and

an output step of outputting a set of information consisting of the validity data and the information to be validated.

22. A program recording medium on which a program to be executed by a computer is recorded, said program comprising:

a validity-data generating step of generating validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information;

a verifying-parameter generating step of generating a verifying parameter for verifying the presence of the secret information;

an information-to-be-validated generating step of generating information to be validated which includes the verifying parameter and which is validated by the validity data; and

an output step of outputting a set of information consisting of the validity data and the information to be validated.

23. An information processing apparatus for processing a set of information which comprises: validity data

including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data, said information processing apparatus comprising:

storage means for storing said set of information;

information-to-be-validated transmission means for transmitting the information to be validated to a checking device for checking the information to be validated; and

verifying-data generating means for generating verifying data for verifying the presence of the secret information and for transmitting the verifying data to said checking device.

24. An information processing apparatus according to claim 23, wherein said set of information is an electronic ticket.

25. An information processing apparatus according to claim 23, further comprising:

first encryption means for encrypting the validity data with a first encryption key; and

first decryption means for decrypting the validity data encrypted with the first encryption key by using the first encryption key,

wherein said storage means stores the validity data encrypted with the first encryption key.

26. An information processing apparatus according to claim 25, wherein the first encryption key is updated with a predetermined timing.

27. An information processing apparatus according to claim 25, further comprising:

second encryption means for encrypting the first encryption key with a second encryption key; and

second decryption means for decrypting the first encryption key encrypted with the second encryption key by using the second encryption key,

wherein said storage means also stores the first encryption key encrypted with the second encryption key.

28. An information processing apparatus according to claim 27, wherein the second encryption key is integrated into hardware which forms said second encryption means and said second decryption means.

29. An information processing apparatus according to claim 27, wherein the second encryption key is updated with a predetermined timing.

30. An information processing apparatus according to claim 24, wherein the information to be validated further includes content of rights associated with the electronic ticket.

31. An information processing apparatus according to claim 24, wherein the information to be validated is processed so as to be prevented from being tampered with.

32. An information processing apparatus according to claim 31, wherein the information to be validated includes a digital signature so as to be prevented from being tampered with.

33. An information processing apparatus according to claim 24, wherein the secret information is a secret key used in a public key cryptosystem, and the verifying parameter is a public key corresponding to the secret key, and said verifying-data generating means generates the verifying data by performing processing using the secret key.

34. An information processing apparatus according to claim 33, wherein the validity data includes the number of uses of the electronic ticket, and said verifying-data generating means processes predetermined information and the number of uses with the secret key, and sends a processing result and the number of uses.

35. An information processing apparatus according to claim 34, further comprising incrementing means for incrementing the number of uses contained in the validity data stored in said storage means every time said verifying-data generating means sends the number of uses.

36. An information processing apparatus according to claim 24, further comprising assigning means for assigning information of the electronic ticket to an external device.

37. An information processing apparatus according to claim 36, further comprising authentication means for performing authentication processing with said external device when assigning the electronic ticket information to said external device.

38. An information processing apparatus according to claim 36, wherein said assigning means encrypts the validity

data of the electronic ticket and sends the encrypted validity data to said external device.

39. An information processing apparatus according to claim 38, wherein said assigning means sends a device certificate to said external device, said device certificate including a public key used in a public key cryptosystem, and a digital signature generated by a predetermined certifying center for the public key so as to certify that said information processing apparatus is a legal device, and said assigning means decrypts, by using a secret key corresponding to the public key, an encryption key which is encrypted with the public key contained in the device certificate and which is sent from said external device, and encrypts the validity data with the decrypted encryption key.

40. An information processing apparatus according to claim 36, wherein said assigning means assigns the electronic ticket information to said external device and also deletes the electronic ticket information from said storage means.

41. An information processing apparatus according to claim 24, further comprising assignment-receiving means for receiving information of the electronic ticket from an

external device.

42. An information processing apparatus according to claim 41, further comprising authentication means for performing authentication processing with said external device when receiving the electronic ticket information.

43. An information processing apparatus according to claim 42, wherein said assignment-receiving means verifies the validity of the information to be validated sent from said external device.

44. An information processing apparatus according to claim 43, wherein the information to be validated further comprises an issuer certificate including issuer identifying information for identifying an issuer of the electronic ticket, a public key for verifying the issuer, and a digital signature generated by a predetermined certifying center for the issuer identifying information and the public key, thereby certifying the issuer of the electronic ticket, and said assignment-receiving means verifies the validity of the information to be validated based on the issuer certificate.

45. An information processing apparatus according to claim 43, wherein the information to be validated includes a

digital signature, and said assignment-receiving means verifies the validity of the information to be validated based on the digital signature.

46. An information processing apparatus according to claim 44, wherein the information to be validated includes a digital signature generated by a secret key corresponding to the public key, and said assignment-receiving means verifies the validity of the information to be validated by processing the digital signature with the public key.

47. An information processing apparatus according to claim 41, wherein said assignment-receiving means receives the encrypted validity data.

48. An information processing apparatus according to claim 47, wherein said assignment-receiving means receives a device certificate including a public key used in a public key cryptosystem, and a digital signature generated by a predetermined certifying center for the public key so as to certify that said external device is a legal device, and said assignment-receiving means sends a predetermined encryption key encrypted with the public key contained in the device certificate to said external device, and receives the validity data encrypted with the predetermined

encryption key.

49. An information processing method for processing a set of information which comprises: validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data, said information processing method comprising:

an information-to-be-validated transmission step of transmitting the information to be validated to a checking device for checking the information to be validated; and

a verifying-data generating step of generating verifying data for verifying the presence of the secret information and for transmitting the verifying data to said checking device.

50. A program recording medium for recording a program which controls a computer to process a set of information, said set of information comprising: validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said

validity data being used for verifying the validity of information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data, said program comprising:

an information-to-be-validated transmission step of transmitting the information to be validated to a checking device for checking the information to be validated; and

a verifying-data generating step of generating verifying data for verifying the presence of the secret information and for transmitting the verifying data to said checking device.

51. An information processing apparatus for checking a set of information which comprises: validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data, said information processing apparatus comprising:

information-to-be-validated receiving means for receiving the information to be validated from an external

device;

verifying-data receiving means for receiving verifying data for verifying the presence of the secret information from said external device; and

presence determining means for determining the presence of the secret information in said external device by using the verifying data and the verifying parameter contained in the information to be validated.

52. An information processing apparatus according to claim 51, wherein said set of information is an electronic ticket.

53. An information processing apparatus according to claim 52, wherein the information to be validated further includes content of rights associated with the electronic ticket, and said information processing apparatus further comprises right determining means for determining whether the content of rights satisfies predetermined service providing conditions.

54. An information processing apparatus according to claim 52, wherein:

the secret information is a secret key used in a public key cryptosystem;

the verifying parameter is a public key corresponding to the secret key;

the verifying data is generated by processing using the secret key contained in the validity data; and

said presence determining means determines the presence of the secret key by processing the verifying data with the public key.

55. An information processing apparatus according to claim 54, wherein the validity data includes the number of uses of the electronic ticket, and the verifying data is formed of the number of uses and a processing result obtained by processing predetermined information and the number of uses with the secret key.

56. An information processing apparatus according to claim 52, further comprising checking means for checking the validity of the information to be validated sent from said external device.

57. An information processing apparatus according to claim 56, wherein the information to be validated further comprises an issuer certificate information including issuer identifying information for identifying an issuer of the electronic ticket, a public key for verifying the issuer,

and a digital signature generated by a predetermined certifying center for the issuer identifying information and the public key, thereby certifying the issuer of the electronic ticket, and said checking means checks the validity of the information to be validated based on the issuer certificate.

58. An information processing apparatus according to claim 56, wherein the information to be validated includes a digital signature, and said checking means checks the validity of the information to be validated based on the digital signature.

59. An information processing apparatus according to claim 57, wherein the information to be validated includes a digital signature generated by a secret key corresponding to the public key, and said checking means checks the validity of the information to be validated by processing the digital signature with the public key.

60. An information processing method for checking a set of information which comprises: validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of

information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said validity data, said information processing method comprising:

an information-to-be-validated receiving step of receiving the information to be validated from an external device;

a verifying-data receiving step of receiving verifying data for verifying the presence of the secret information from said external device; and

a presence determining step of determining the presence of the secret information in said external device by using the verifying data and the verifying parameter contained in the information to be validated.

61. A program recording medium for recording a program which controls a computer to perform processing for checking a set of information which comprises: validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information; and information to be validated, including a verifying parameter for verifying the presence of the secret information, said information being validated by said

validity data, said program comprising:

an information-to-be-validated receiving step of receiving the information to be validated from an external device;

a verifying-data receiving step of receiving verifying data for verifying the presence of the secret information from said external device; and

a presence determining step of determining the presence of the secret information in said external device by using the verifying data and the verifying parameter contained in the information to be validated.

62. An information processing system comprising a first information processing apparatus, a second information processing apparatus, and a third information processing apparatus,

said first information processing apparatus comprising:

validity-data generating means for generating validity data including secret information to which an algorithm whose presence is verifiable without being exposed is applicable, said validity data being used for verifying the validity of information;

verifying-parameter generating means for generating a verifying parameter for verifying the presence of the secret information;

information-to-be-validated generating means for generating information to be validated which includes the verifying parameter and which is validated by the validity data; and

output means for outputting a set of information consisting of the validity data and the information to be validated,

said second information processing apparatus comprising:

storage means for storing said set of information;

information-to-be-validated transmission means for transmitting the information to be validated to said third information processing apparatus for checking the information to be validated; and

verifying-data generating means for generating verifying data for verifying the presence of the secret information and for transmitting the verifying data to said third information processing apparatus,

said third information processing apparatus comprising:

information-to-be-validated receiving means for receiving the information to be validated from said second information processing apparatus;

verifying-data receiving means for receiving the verifying data for verifying the presence of the secret information from said second information processing

apparatus; and

presence determining means for determining the presence of the secret information in said second information processing apparatus by using the verifying data and the verifying parameter contained in the information to be validated.